Journal of Combinatorial Theory, Series A **100**, 116–135 (2002)
doi:10.1006/jcta.2002.3283

Circulant 16-Modular Hadamard Matrices and Jacobi Sums

Shalom Eliahou[1]

Département de Mathématiques, LMPA Joseph Liouville, Université du Littoral Côte d'Opale, Bâtiment Poincaré, 50, rue Ferdinand Buisson, B.P. 699, 62228 Calais, France
E-mail: eliahou@lmpa.univ-littoral.fr

and

Michel Kervaire

Département de Mathématiques, Université de Genève, 2-4, rue du Lièvre, B.P. 240, 1211 Genève 24, Suisse, Switzerland
E-mail: Michel.Kervaire@math.unige.ch

Received December 28, 2000; published online July 2, 2002

We are concerned here with the existence problem of 16-modular circulant Hadamard matrices H of size $4p$ (p prime), satisfying the additional condition that any two rows at distance $n/2$ in H are strictly orthogonal. A necessary existence condition is $p \equiv 1 \bmod 8$. For $p \equiv 1 \bmod 16$, existence follows from the more general result of a previous paper of ours, showing the existence of $(p-1)$-modular matrices of the above kind. In the remaining case $p \equiv 9 \bmod 16$, we construct explicit examples which solve the problem whenever 2 is a fourth power mod p. When 2 is not a fourth power mod p, we conjecture that such matrices cannot exist. © 2002 Elsevier Science (USA)

1. INTRODUCTION

Let $m \geqslant 2$ be an integer. An *m-modular* Hadamard *matrix* is a square matrix H of size n, with entries ± 1, satisfying the weakened Hadamard condition

$$H H^t \equiv nI \bmod m,$$

where I stands for the identity matrix of order n.

This notion was introduced by Marrero and Butson in 1972 [MB1,MB2]. As in the classical case, it is conjectured that m-modular Hadamard matrices exist in every size n divisible by 4. The highest modulus for which this problem has been positively answered is currently $m = 32$ [EK1].

[1] To whom correspondence should be addressed.

0097-3165/02 $35.00

In the present paper, we will only be interested in *circulant* modular Hadamard matrices, specifically for the modulus $m = 16$. According to Ryser's conjecture (1963), in the classical case circulant Hadamard matrices are believed not to exist in size $n > 4$. This is no more so however, in the modular context. In [EK2], we have constructed circulant $(p-1)$-modular Hadamard matrices H of size $4p$, where p is a prime number satisfying $p \equiv 1 \bmod 4$. In fact, $H H^t = 4pI + (p-1)M$, where the entries of M have no common divisor > 1. These matrices have the additional property that the $2p$th periodic correlation

$$\gamma_{2p} = \sum_{i \in \mathbf{Z}/4p\mathbf{Z}} a_i a_{i+2p}$$

of their first row $a = (a_0, \ldots, a_{4p-1})$ is (strictly) zero.

Circulant m-modular Hadamard matrices of even size $2n$ with first row $(a_0, a_1, \ldots, a_{2n-1})$ having the property

$$\gamma_n = \sum_{i \in \mathbf{Z}/2n\mathbf{Z}} a_i a_{i+n} = 0$$

will be said to be of *enhanced type*. As explained in [EK2], this condition is designed to rule out certain uninteresting examples.

The $(p-1)$-modular examples of [EK2] naturally provide 16-modular circulant Hadamard matrices of enhanced type whenever $p \equiv 1 \bmod 16$.

As observed in [EK2], no 16-modular circulant Hadamard matrices of enhanced type and length $4p$ may exist for $p \not\equiv 1 \bmod 8$.

In this paper, we consider the remaining case $p \equiv 9 \bmod 16$. We have observed, using machine experimentation, that for certain such primes, for instance $p = 73, 89, \ldots$, a variant of the examples in [EK2] could also produce circulant matrices of size $4p$, which are 16-modular Hadamard matrices of enhanced type, a modulus larger than the expected value 8 which is the best power of 2 dividing $p-1$.

In Theorem 1 we exhibit a family of circulant matrices with entries in $\{\pm 1\}$, of size $4p$ again, where p is a prime congruent 1 mod 8. These matrices are described by specifying their first row $X = (a_0, \ldots, a_{4p-1})$ and explicit formulas are given for the periodic correlations

$$\gamma_k(X) = \sum_{j \in \mathbf{Z}/4p\mathbf{Z}} a_j a_{j+k}, \qquad \text{for } k = 1, \ldots, 4p-1.$$

The formulas involve the integers a and b occurring in the decomposition $p = a^2 + b^2$ of p as a sum of squares.

In the course of the proof of Theorem 1, the integers a and b will be defined by the formula $a + bi = -J(\eta, \chi) \in \mathbf{Z}[i]$, where J is the Jacobi sum

on η, χ, the quadratic and biquadratic characters modulo p, respectively, and $i = \sqrt{-1}$. The definition of Jacobi sums will be recalled as needed in Section 3.

In Theorem 2 the circulant matrices arising from Theorem 1 will be shown to be enhanced 8-modular Hadamard matrices. Not all of them however are 16-modular. Indeed, we completely characterize those primes $p \equiv 1 \bmod 8$ for which this happens: the circulant matrix obtained from Theorem 1 is a 16-modular Hadamard matrix if and only if $p \equiv 9 \bmod 16$ and 2 is a fourth power in $\mathbf{F}_p^*$.

In the proof we shall use a famous theorem of Gauss which states that 2 is a fourth power modulo p if and only if p has a representation $p = a^2 + b^2$ with integers a and b such that b is divisible by 8.

In contrast, for other primes p, for instance $p = 41$, still satisfying the congruence $p \equiv 9 \bmod 16$, but for which 2 is not a fourth power modulo p, machine experimentation seems to indicate that enhanced 16-modular circulant Hadamard matrices of size $4p$ simply do not exist.

2. STATEMENT OF RESULTS

A circulant matrix is specified by its first row $X = (a_0, \ldots, a_{\ell-1})$ which we will write as a "polynomial" $F(z) = \sum_{s \in \mathbf{Z}/\ell\mathbf{Z}} a_s z^s \in \mathbf{Z}[z]/(z^\ell - 1)$, or view equivalently as an element in the group ring $\mathbf{Z}C_\ell$ of the cyclic group of order ℓ generated by z.

In the sequel, we shall consider only sequences $X = (a_0, \ldots, a_{\ell-1})$ which have all their coefficients $a_0, \ldots, a_{\ell-1}$ belonging to $\{\pm 1\}$.

The periodic correlations of X (or F) are by definition

$$\gamma_k(X) = \sum_{i=0}^{\ell-1} a_i a_{i+k},$$

where the indices are read modulo ℓ, for every k $(0 \leqslant k \leqslant \ell - 1)$.

Observe that $\gamma_0(X) = \ell$ and that $\gamma_{\ell-k}(X) = \gamma_k(X)$ for $k = 1, \ldots, \ell - 1$.

Clearly, $\gamma_k(X)$ is the dot product of X with its kth shift $\sigma_k(X)$, where $\sigma_k(X) = (a_k, a_{k+1}, \ldots, a_{k+\ell-1})$, with indices read modulo ℓ.

A circulant matrix $\mathrm{circ}(X)$ is associated to X. The rows of $\mathrm{circ}(X)$ are the shifts $\sigma_{-k}(X)$, $k = 0, \ldots, \ell - 1$ of the sequence X.

Evidently, $\gamma_k(X) \equiv 0 \bmod m$ for all k in the interval $1 \leqslant k \leqslant \frac{\ell}{2}$ means that $H = \mathrm{circ}(X)$ is an m-modular circulant Hadamard matrix.

Hence, in order to describe our modular Hadamard matrices, it will suffice to describe the corresponding sequences (polynomials) with correlations satisfying the appropriate congruences.

Let p be a prime satisfying $p \equiv 1 \bmod 8$ and let $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ be the finite field with p elements.

We fix a generator c of the (cyclic) group $\mathbf{F}_p^*$. Let $\Gamma \subset \mathbf{F}_p^*$ be the cyclic subgroup of $\mathbf{F}_p^*$ of order $\frac{p-1}{4}$ generated by c^4. The group Γ is the unique subgroup of index 4 in $\mathbf{F}_p^*$.

The sets $c^v\Gamma$, for $v = 0, 1, 2, 3$ are the four cosets of Γ in $\mathbf{F}_p^*$. Let the set S stand for the union of the two disjoint intervals of integers $1 \leqslant s \leqslant p-1$ and $p+1 \leqslant s \leqslant 2p-1$, that is $S = [1, p-1] \cup [p+1, 2p-1]$. We denote by ϖ the natural projection $\varpi : S \to \mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$, i.e. reduction modulo p.

Let $\Gamma_v \subset S$, $v = 0, 1, 2, 3$ be the inverse images

$$\Gamma_v = \varpi^{-1}(c^v\Gamma).$$

The four subsets $\Gamma_v \subset S$, $v = 0, 1, 2, 3$ form a partition of S into subsets of equal cardinality $|\Gamma_v| = \frac{p-1}{2}$.

We denote by C_{4p} the cyclic group of order $4p$ with generator $z \in C_{4p}$ and let $f_v(z)$ be the Hall polynomial of Γ_v, that is $f_v(z) = \sum_{s\in\Gamma_v} z^s$.

Actually, we will use the polynomials

$$A_v = f_v(z^2) = \sum_{s\in\Gamma_v} z^{2s} \qquad \text{and} \qquad B_v = f_v(-z^2) = \sum_{s\in\Gamma_v} (-1)^s z^{2s}.$$

An important role will be played by the decomposition $p = a^2 + b^2$, with a, b integers, which exists since $p \equiv 1 \bmod 4$. As is well known this decomposition is unique up to the signs of a and b if we require a to be odd (and thus b even).

During the proof of Theorem 1 (in the next section), a and b will be defined explicitly, thereby resolving the ambiguity on signs.

It will turn out (in the proof of Theorem 2 in Section 4) that the sign of a occurring in the formulas below, is in fact determined by the requirement $a \equiv 1 \bmod 4$. The sign of b will be essentially irrelevant.

THEOREM 1. *Let p be a prime satisfying $p \equiv 1 \bmod 8$. For any choice of the parameters $\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3$, with values ± 1, we set*

$$\begin{aligned} F(z) = {} & \varepsilon_0(1 + z^{2p} - A_0 - A_2) + \varepsilon_1(A_0 - A_2)z^p \\ & + \varepsilon_2(1 - z^{2p} - B_1 - B_3)z^p + \varepsilon_3(B_1 - B_3). \end{aligned}$$

This polynomial $F(z) \in \mathbf{Z}[z]/(z^{4p} - 1)$ has all its coefficients equal to ± 1 and satisfies an identity

$$F(z)F(z^{-1}) = 4p + \sum_{k=1}^{2p-1} \gamma_k(z^k + z^{-k}) \in \mathbf{Z}[z]/(z^{4p} - 1),$$

where the correlations γ_k *for* $1 \leqslant k \leqslant 2p-1$, $k \neq p$ *are given by*

$$\gamma_k = \begin{cases} p-9 & \text{if } k = 4j \quad \text{with} \quad 1 \leqslant j \leqslant \frac{p-1}{2}, \\ \pm 2(a+3) & \text{if } k = 4j-2 \quad \text{with} \quad 1 \leqslant j \leqslant \frac{p-1}{2}, \\ \pm 2(a+3) & \text{if } k = 2j-1 \quad \text{with} \quad 1 \leqslant j \leqslant p, \\ & \quad \text{and } k \text{ is quadratic residue mod } p, \\ \pm 2b & \text{if } k = 2j-1 \quad \text{with} \quad 1 \leqslant j \leqslant p, \\ & \quad \text{and } k \text{ is not quadratic residue mod } p. \end{cases}$$

The signs in front of $\pm 2(a+3)$ *and* $\pm 2b$ *are specified in formulas* (11) *and* (12) at the end of Section 3.

In addition, $\gamma_p = 0$.

Note that the formulation of the theorem contains, in particular, the statement $\gamma_{2p} = 0$.

The integers a and b will be defined in the course of the proof in the next section by the explicit formula $a + bi = -J(\eta, \chi)$, where $J(\eta, \chi)$ is the Jacobi sum on the quadratic and biquadratic characters modulo p, respectively. They satisfy $p = a^2 + b^2$.

It follows from the above theorem that circulant enhanced 16-modular Hadamard matrices of size $4p$ exist even for $p \equiv 9 \bmod 16$ if p is a prime whose decomposition $p = a^2 + b^2$ (normalized by $a + bi = -J(\eta, \chi)$) satisfies $a \equiv -3 \bmod 8$ and $b \equiv 0 \bmod 8$.

Our next result will relate the divisibility by 16 of the correlations arising in Theorem 1 to the theorem of Gauss about the biquadratic character of 2 in the field $\mathbf{F}_p^*$.

THEOREM 2. *Let* p *be a prime congruent* $1 \bmod 8$. *The circulant matrix determined by the polynomial* $F(z)$ *in Theorem* 1 *is an enhanced* 8*-modular Hadamard matrix of size* $4p$. *It is a* 16*-modular Hadamard matrix if and only if* $p \equiv 9 \bmod 16$ *and* 2 *is a fourth power in* $\mathbf{F}_p^*$.

It will become apparent during the proof of Theorem 2 in Section 4 that the choice of sign in $a + bi = -J(\eta, \chi)$, is equivalent to the normalization of the sign of the odd integer a by the requirement $a \equiv 1 \bmod 4$.

We now proceed to the proofs.

3. PROOF OF THEOREM 1

The assertion about the coefficients of $F(z)$ is simple enough to prove by reducing modulo 2 and recalling that $\Gamma_0 \cup \Gamma_1 \cup \Gamma_2 \cup \Gamma_3$ is a partition of $S = [1, p-1] \cup [p+1, 2p-1]$. The details are left to the reader.

The calculation of $F(z)F(z^{-1})$ will be divided into 4 steps.

Step 1. We prove first that $F(z)F(z^{-1})$ has the form $F(z)F(z^{-1}) = C + C_{0,1}\varepsilon_0\varepsilon_1$, where

$$C = 4 + 2\{(A_0^2 - 2A_0) + (A_2^2 - 2A_2) + (B_1^2 - 2B_1) + (B_3^2 - 2B_3)\} \quad (1)$$

and

$$C_{0,1} = \{(A_2^2 - 2A_2) - (A_0^2 - 2A_0)\}(z^p + z^{-p}). \quad (2)$$

This statement is derived from the symmetry properties of the sets Γ_v.

The 4 sets Γ_v, $v = 0, 1, 2, 3$ are stable under the involutions φ and ρ of the set S defined, respectively, by the formulas

$$\varphi(x) = 2p - x$$

and

$$\rho(x) = \begin{cases} p - x & \text{if } x \in [1, p-1], \\ 3p - x & \text{if } x \in [p+1, 2p-1]. \end{cases}$$

Note that indeed $-1 \in \Gamma$ because we have $-1 = c^{(p-1)/2} = (c^4)^{(p-1)/8} \in \Gamma$ and thus $x \in \Gamma_v$ implies $\varphi(x) \in \Gamma_v$ and $\rho(x) \in \Gamma_v$.

The set Γ_v being stable under φ, the existence of $\varphi : \Gamma_v \to \Gamma_v$ implies the following properties of the sums $\sum_{s\in\Gamma_v} z^{2s}$ as well as $\sum_{s\in\Gamma_v} (-1)^s z^{2s}$:

$$\sum_{s\in\Gamma_v} z^{-2s} = \sum_{s\in\Gamma_v} z^{2s}, \qquad \sum_{s\in\Gamma_v} (-1)^s z^{-2s} = \sum_{s\in\Gamma_v} (-1)^s z^{2s} \quad (3)$$

for $v = 0, 1, 2, 3$.

This follows simply by applying the involution φ to the summation index s, using $z^{4p} = 1$ and means that $f_v(z^2)$ and $f_v(-z^2)$ for $i = 0, 1, 2, 3$ are all self-reciprocal polynomials.

The existence of the automorphisms $\rho : \Gamma_v \to \Gamma_v$ for $i = 0, 1, 2, 3$ implies the following formulas:

$$(1 - z^{2p})A_v = 0, \qquad (1 + z^{2p})B_v = 0. \quad (4)$$

Recalling the definitions of A_v, B_v above, these formulas amount to

$$\sum_{s\in\Gamma_v} z^{2s} = z^{2p} \sum_{s\in\Gamma_v} z^{2s}, \qquad \sum_{s\in\Gamma_v} (-1)^s z^{2s} = -z^{2p} \sum_{s\in\Gamma_v} (-1)^s z^{2s}.$$

For the proofs, note that

$$\sum_{s\in\Gamma_v}(-1)^s z^{2s} = \sum_{s\in\Gamma_v}(-1)^{\rho(s)} z^{2\rho(s)}$$
$$= \sum_{s\in\Gamma_v\cap[1,p-1]}(-1)^{p-s} z^{2(p-s)} + \sum_{s\in\Gamma_v\cap[p+1,2p-1]}(-1)^{3p-s} z^{2(3p-s)}.$$

Still remembering that $z^{4p}=1$, we obtain

$$\begin{aligned}\sum_{s\in\Gamma_v}(-1)^s z^{2s} &= -z^{2p}\sum_{s\in\Gamma_v}(-1)^s z^{-2s}\\ &= -z^{2p}\sum_{s\in\Gamma_v}(-1)^{(2p-s)} z^{2(2p-s)}\\ &= -z^{2p}\sum_{s\in\Gamma_v}(-1)^s z^{2s},\end{aligned}$$

using again the automorphism φ above.

The proof of the formula without the sign is the same.

As a corollary, we get

$$f_\mu(z^2)f_\nu(-z^2) = A_\mu B_\nu = 0, \tag{5}$$

obtained by observing that $(1-z^{2p})$ and $(1+z^{2p})$ both kill the above product. The first factor is killed by $1-z^{2p}$. The second by $1+z^{2p}$. It follows that $2=(1+z^{2p})+(1-z^{2p})$ annihilates the left-hand side of (3) which must be 0 since 2 is not a divisor of zero in $\mathbf{Z}C_{4p}$.

Consequently, the terms in $F(z)F(z^{-1})$ involving the factors $\varepsilon_0\varepsilon_2,\ \varepsilon_0\varepsilon_3,\ \varepsilon_1\varepsilon_2,\ \varepsilon_1\varepsilon_3$ all vanish.

Indeed, these terms are, respectively,

$$\begin{aligned}&\varepsilon_0\varepsilon_2(1+z^{2p}-A_0-A_2)(1-z^{2p}-B_1-B_3)(z^p+z^{-p})=0,\\ &2\varepsilon_0\varepsilon_3(1+z^{2p}-A_0-A_2)(B_1-B_3)=0,\\ &2\varepsilon_1\varepsilon_2(A_0-A_2)(1-z^{2p}-B_1-B_3)=0,\\ &\varepsilon_1\varepsilon_3(A_0-A_2)(B_1-B_3)(z^p+z^{-p})=0.\end{aligned}$$

Moreover, we also have

$$\varepsilon_2\varepsilon_3(1-z^{2p}-B_1-B_3)(B_1-B_3)(z^p+z^{-p})=0,$$

since $(B_1-B_3)(z^p+z^{-p}) = (B_1-B_3)(1+z^{2p})z^{-p}=0$.

Hence, there remains only $F(z)F(z^{-1}) = C + C_{0,1}\varepsilon_0\varepsilon_1$, with

$$C = (1 + z^{2p} - A_0 - A_2)^2 + (A_0 - A_2)^2 + (1 - z^{2p} - B_1 - B_3)^2 + (B_1 - B_3)^2,$$
$$C_{0,1} = (1 + z^{2p} - A_0 - A_2)(A_0 - A_2)(z^p + z^{-p}).$$

Recalling that $z^{2p}A_v = A_v$ and $z^{2p}B_v = -B_v$, a short calculation yields the alleged formulas (1) and (2):

$$C = 4 + 2\{(A_0^2 - 2A_0) + (A_2^2 - 2A_2) + (B_1^2 - 2B_1) + (B_3^2 - 2B_3)\}$$

and

$$C_{0,1} = \{(A_2^2 - 2A_2) - (A_0^2 - 2A_0)\}(z^p + z^{-p}).$$

It remains to evaluate $A_0^2, A_2^2, B_1^2, B_3^2$.

The next step will consist in evaluating A_0, A_1, A_2 and A_3 from a linear system in the group ring of C_{4p} over the ring of Gaussian integers $\mathbf{Z}[\mu_4] = \mathbf{Z}[i]$, where $i = \sqrt{-1}$.

That is, we will regard $\mathbf{Z}C_{4p}$ as a subring of $\mathbf{Z}[i]C_{4p}$.

Step 2. Calculation of A_0, A_1, A_2 and A_3 by a linear system in $\mathbf{Z}[i]$.

To begin with, we have

$$A_0 + A_2 + A_1 + A_3 = T - (1 + z^{2p}), \tag{6}$$

where $T = \sum_{s=0}^{2p-1} z^{2s}$.

On the other hand, note that $\Gamma_0 \cup \Gamma_2$ is the set of squares modulo $2p$ and $\Gamma_1 \cup \Gamma_3$ the set of non-squares. Hence, we have

$$A_0 + A_2 - A_1 - A_3 = \sum_{s \in S} \left(\frac{s}{p}\right) z^{2s} = \left(\sum_{s=1}^{p-1} \left(\frac{s}{p}\right) z^{2s}\right)(1 + z^{2p}),$$

where $(\frac{s}{p})$ is the Legendre symbol.

In order to write down the necessary additional linear equations involving A_0, A_1, A_2 and A_3, we need some notation.

Let ψ be an arbitrary multiplicative character, that is a homomorphism $\psi : \mathbf{F}_p^* \to \mu_{p-1} \subset \mathbf{C}^*$ to the multiplicative subgroup of $(p-1)$th roots of unity μ_{p-1}. We introduce the sum

$$G(\psi) = \sum_{s=1}^{p-1} \psi(\varpi(s)) z^{2s} \in \mathbf{Z}[\mu_{p-1}][z]/(z^{4p} - 1),$$

where $\varpi : [1, p-1] \to \mathbf{F}_p^*$ is reduction modulo p (which we will occasionally suppress from the notation).

Hence, we can write

$$A_0 + A_2 - A_1 - A_3 = \left(\sum_{s=1}^{p-1} \left(\frac{s}{p}\right) z^{2s}\right)(1 + z^{2p}) = G(\eta)(1 + z^{2p}), \qquad (7)$$

where η is the quadratic character given by the Legendre symbol $\eta(x) = \left(\frac{x}{p}\right)$.

We denote by $\mu_4 = \{1, i, -1, -i\} \subset \mathbf{Z}[i]$ the group of units generated by i and let $\chi\colon \mathbf{F}_p^* \to \mu_4$ be the multiplicative homomorphism determined by $\chi(c) = i$, where c is a generator of $\mathbf{F}_p^*$ as above. Note that $\Gamma = \ker(\chi)$. By abuse of notation, we also denote with the same letter χ, the composition

$$[1, p-1] \cup [p+1, 2p-1] \xrightarrow{\varpi} \mathbf{F}_p^* \xrightarrow{\chi} \mu_4,$$

where ϖ as above is reduction modulo p.

Since $\Gamma_0 \cup \Gamma_1 \cup \Gamma_2 \cup \Gamma_3 = [1, p-1] \cup [p+1, 2p-1]$, we have

$$A_0 + iA_1 - A_2 - iA_3 = \sum_{s=1}^{p-1} \chi(s) z^{2s} + \sum_{s=p+1}^{2p-1} \chi(s) z^{2s}.$$

Since χ is periodic of period p, we have

$$A_0 + iA_1 - A_2 - iA_3 = \left(\sum_{s=1}^{p-1} \chi(s) z^{2s}\right)(1 + z^{2p}).$$

Thus, we write

$$A_0 + iA_1 - A_2 - iA_3 = G(\chi)(1 + z^{2p}), \qquad (8)$$

as an element of $\mathbf{Z}[i][z]/(z^{4p} - 1)$.

We view Eqs. (6), (7) and the pair of equations consisting of (8) plus its complex conjugate as a linear system of 4 equations in the unknown A_0, A_2, A_1, A_3 over the ring $\mathbf{Z}[i][z]/(z^{4p} - 1)$.

This system is easy enough to solve. The formulas for $A_v,\ v = 0, 1, 2, 3$ can be unified into the single expression

$$4A_v = T + \{-1 + (-1)^v G(\eta) + \bar{\chi}(c^v) G(\chi) + \chi(c^v) G(\bar{\chi})\}(1 + z^{2p}), \qquad (9)$$

for $v = 0, 1, 2, 3$, all well-defined elements of $\mathbf{Z}[i][z]/(z^{4p} - 1)$.

In Step 4 we will calculate directly $A_0^2, A_1^2, A_2^2, A_3^2$ from these formulas. In order to get B_1^2, B_3^2 which are needed for the calculation of

$$C = 4 + 2(A_0^2 - 2A_0) + 2(A_2^2 - 2A_2) + 2(B_1^2 - 2B_1) + 2(B_3^2 - 2B_3),$$

in the expression $F(z)F(z^{-1}) = C + C_{0,1}\varepsilon_0\varepsilon_1$ given by formulas (1) and (2), we observe that there is a ring automorphism σ of $\mathbf{Z}[i][z]/(z^{4p}-1)$ determined by $\sigma|_{\mathbf{Z}[i]} = id.$ and $\sigma(z) = iz$, with the property $\sigma(A_v) = B_v$.

Step 3. In order to calculate A_v^2 from formula (9) giving A_v, we shall need to evaluate products of the sums $G(\psi)$. For this purpose, we require some notation and a lemma which we now proceed to state and prove.

For any multiplicative character $\psi : \mathbf{F}_p^* \to \mu_{p-1} \subset \mathbf{C}^*$, set

$$g(\psi) = \sum_{x \in \mathbf{F}_p^*} \psi(x) w^x \in \mathbf{C}[w]/(w^p - 1).$$

As usual, the trivial character ε is defined by $\varepsilon(x) = 1$ for all $x \in \mathbf{F}_p^*$. Also, $\bar{\psi}$ is the character defined by $\bar{\psi}(x) = \overline{\psi(x)}$. Note that $\bar{\psi}(x) = \psi(x^{-1})$ since the values of ψ are roots of unity. The characters form a group under the multiplication $\vartheta\psi(x) = \vartheta(x)\psi(x)$.

LEMMA. *Let $\vartheta, \psi : \mathbf{F}_p^* \to \mathbf{C}^*$ be two multiplicative characters and let g be defined as above. We have*:

(1) *If ψ is not the trivial character, then*

$$g(\psi)g(\bar{\psi}) = \psi(-1)\left(p - 1 - \sum_{s=1}^{p-1} w^s\right).$$

(2) *If ψ and ϑ are two characters such that $\vartheta \neq \bar{\psi}$, then*

$$g(\vartheta)g(\psi) = J(\vartheta, \psi)g(\vartheta\psi),$$

where $J(\vartheta, \psi)$ is the Jacobi sum $\sum_{x \in \mathbf{F}_p^* \setminus \{1\}} \vartheta(x)\psi(1-x)$.

This lemma is well known in the classical context where w is replaced by a pth root of unity. See for example [IR, Chap. 8, pp. 92–94]. Note that if a primitive pth root of unity ζ is substituted for w, then part (1) above becomes $g_\zeta(\psi)g_\zeta(\bar{\psi}) = \psi(-1)p$, where $g_\zeta(\psi) = \sum_{x \in \mathbf{F}_p^*} \psi(x)\zeta^x$, as is well known.

The proof in our setting is essentially the same as in the classical case and will be repeated here as a brief sketch only.

For the proof of part (1) of the lemma, we have

$$g(\psi)g(\bar{\psi}) = \sum_{x,y \in \mathbf{F}_p^*} \psi(xy^{-1}) w^{x+y}.$$

For each fixed $y \in \mathbf{F}_p^*$, we replace the summation index x by $-xy$ and obtain

$$\begin{aligned} g(\psi)g(\bar{\psi}) &= \sum_{x,y\in\mathbf{F}_p^*} \psi(-xyy^{-1})w^{(1-x)y} \\ &= \psi(-1)\sum_{x,y\in\mathbf{F}_p^*} \psi(x)w^{(1-x)y}. \end{aligned}$$

For $x = 1$, all terms $w^{(1-x)y}$ equal $1 \in \mathbf{C}[w]/(w^p - 1)$ independently of $y \in \mathbf{F}_p^*$.

For any fixed $x \in \mathbf{F}_p^*\backslash\{1\}$, we have $\sum_{y\in\mathbf{F}_p^*} w^{(1-x)y} = \sum_{y\in\mathbf{F}_p^*} w^y$, replacing the summation index y by $\frac{y}{1-x}$.

Therefore,

$$g(\psi)g(\bar{\psi}) = \psi(-1)\left\{\sum_{y\in\mathbf{F}_p^*} \psi(1) + \sum_{x\in\mathbf{F}_p^*\backslash\{1\}} \psi(x)\sum_{y\in\mathbf{F}_p^*} w^y\right\}.$$

Now, $\sum_{x\in\mathbf{F}_p^*} \psi(x) = 0$ since ψ is non-trivial by hypothesis. It follows that $\sum_{x\in\mathbf{F}_p^*\backslash\{1\}} \psi(x) = -1$ and

$$g(\psi)g(\bar{\psi}) = \psi(-1)\left(p - 1 - \sum_{x\in\mathbf{F}_p^*} w^x\right),$$

as announced.

As to part (2), we follow Ireland and Rosen [IR, p. 94].

Notice that

$$g(\vartheta)g(\psi) = \sum_{x,y\in\mathbf{F}_p^*} \vartheta(x)\psi(y)z^{x+y} = \sum_t \left(\sum_{x+y=t} \vartheta(x)\psi(y)\right)z^t,$$

where x, y are restricted to $\mathbf{F}_p^*$ in the second summation also.

If $t = 0$, then

$$\sum_{x+y=t} \vartheta(x)\psi(y) = \sum_{x\in\mathbf{F}_p^*} \vartheta(x)\psi(-x) = \psi(-1)\sum_{x\in\mathbf{F}_p^*} \vartheta\psi(x) = 0,$$

since $\vartheta\psi \neq \varepsilon$ (the trivial character) by assumption.

If $t \neq 0$, define x' and y' by $x = tx'$ and $y = ty'$. If $x + y = t$, then $x' + y' = 1$. It follows that, for fixed $t \neq 0$,

$$\sum_{x+y=t} \vartheta(x)\psi(y) = \sum_{x'+y'=1} \vartheta(tx')\psi(ty') = \vartheta\psi(t)J(\vartheta,\psi).$$

Substituting this into the equation above for $g(\vartheta)g(\psi)$ yields

$$g(\vartheta)g(\psi) = \sum_{t\in\mathbf{F}_p^*} \vartheta\psi(t)J(\vartheta,\psi)z^t = J(\vartheta,\psi)g(\vartheta\psi). \quad \blacksquare$$

We apply the lemma with $\chi\colon \mathbf{F}_p^* \to \mu_4 = \{1, i, -1, -i\} \subset \mathbf{C}^*$ the biquadratic character determined by $\chi(c) = i$, the same as considered above with $\ker(\chi) = \Gamma$. We also use the quadratic character which we denote by $\eta\colon \mathbf{F}_p^* \to \mu_2 = \{1, -1\} \subset \mathbf{C}^*$ given by the Legendre symbol: $\eta(x) = (\frac{x}{p})$. Note that $\chi^2 = \eta$.

Since $g_\zeta(\eta\chi)$, $g_\zeta(\eta)$, and $g_\zeta(\chi)$ all have absolute value p, it follows that the same holds for $J(\eta,\chi)$. Hence, setting $\pi = -J(\eta,\chi)$ and $\pi = a + bi$, we have $p = \pi\bar{\pi} = a^2 + b^2$. The choice of sign for π is to a large extent arbitrary. We follow the usual convention which is dictated by considerations having to do with the law of biquadratic reciprocity. (see [IR, Chap. 9]). We apologize to the reader who would find this sign convention artificial here.

Before we start using the lemma for the calculations of A_v^2, we recall the equality $J(\chi,\chi) = \chi(-1)J(\eta,\chi)$ which will be used below. It is an immediate corollary to the lemma.

COROLLARY. *If χ and η denote the biquadratic and the quadratic characters, respectively, as above, then $J(\chi,\chi) = \chi(-1)J(\eta,\chi)$.*

Proof. By part (2) of the lemma applied to $\vartheta = \psi = \chi$, we have $J(\chi,\chi) = \frac{g(\chi)^2}{g(\eta)}$. On the other hand, $J(\eta,\chi) = \frac{g(\eta)g(\chi)}{g(\eta\chi)} = \frac{g(\eta)g(\chi)^2}{g(\chi)g(\bar{\chi})}$, observing that $\bar{\chi} = \chi^3 = \eta\chi$ since χ is of order 4 and $\chi^2 = \eta$.

Now, it follows from part (1) of the lemma that $g(\chi)g(\bar{\chi}) = \chi(-1)g(\eta)^2$, since $\bar{\eta} = \eta$ and $\eta(-1) = 1$.

Hence, $J(\eta,\chi) = \frac{g(\eta)g(\chi)^2}{\chi(-1)g(\eta)^2} = \frac{g(\chi)^2}{\chi(-1)g(\eta)} = \frac{J(\chi,\chi)}{\chi(-1)}$. $\blacksquare$

After this digression, we come back to the calculation of the products of sums $G(\psi) = \sum_{s=1}^{p-1} \psi(\varpi(s))z^{2s} \in \mathbf{Z}[\mu_{p-1}][z]/(z^{4p} - 1)$. The statement we need is similar to the above lemma.

The formulas of the lemma translate for $G(\vartheta)$ and $G(\psi)$ to the following statements.

PROPOSITION. *Let ϑ and ψ be multiplicative characters $\vartheta, \psi\colon \mathbf{F}_p^* \to \mathbf{C}^*$.*

(1′) If ψ is not the trivial character, then $G(\psi)G(\bar{\psi})(1 + z^{2p}) = \psi(-1)(p - 1 - t)(1 + z^{2p})$, where $t = \sum_{s=1}^{p-1} z^{2s}$.

(2′) If ψ and ϑ are two characters such that $\vartheta \neq \bar{\psi}$, then $G(\vartheta)G(\psi)(1 + z^{2p}) = J(\vartheta,\psi)G(\vartheta\psi)(1 + z^{2p})$.

Proof. Let proj : $\mathbf{Z}[\mu_{p-1}][z]/(z^{4p}-1) \to \mathbf{Z}[\mu_{p-1}][z]/(z^{2p}-1)$ be the natural projection induced by the identity mapping of $\mathbf{Z}[\mu_{p-1}][z]/(z^{4p}-1)$.

We view the ring $\mathbf{Z}[\mu_{p-1}][w]/(w^p-1)$ as a subring of $\mathbf{Z}[\mu_{p-1}][z]/(z^{2p}-1)$ with the imbedding given by $w = z^2$.

With the ensuing notation, the element $g(\psi) = \sum_{x\in\mathbf{F}_p^*} \psi(x) z^{2x}$ is the image of $G(\psi) \in \mathbf{Z}[\mu_{p-1}][z]/(z^{4p}-1)$ by the projection proj we have just introduced.

Using the above lemma, it follows that

$$G(\psi)G(\bar{\psi}) - \psi(-1)\left(p - 1 - \sum_{s=1}^{p-1} z^{2s}\right)$$

and

$$G(\vartheta)G(\psi) - J(\vartheta,\psi)G(\vartheta\psi),$$

both belong to $\ker(\text{proj}) \subset \mathbf{Z}[\mu_{p-1}][z]/(z^{4p}-1)$ under the hypotheses of the Proposition ($\psi \neq \varepsilon$ for $(1')$ and $\vartheta\psi \neq \varepsilon$ for $(2')$).

The kernel of proj is the ideal $(1-z^{2p})\mathbf{Z}[\mu_{p-1}][z]/(z^{4p}-1)$ generated by $(1-z^{2p})$. This ideal is annihilated under multiplication by $(1+z^{2p})$ since $(1-z^{2p})(1+z^{2p}) = 1 - z^{4p} = 0$ in $\mathbf{Z}[\mu_{p-1}][z]/(z^{4p}-1)$. The proposition follows. ∎

Step 4. We can now calculate the squares A_v^2 using the above formula (9) for A_v.

Observe that $z^2 T = T$, and thus $T^2 = 2pT$.

Similarly we have $TG(\eta) = TG(\chi) = TG(\bar{\chi}) = 0$, where G evaluated on a multiplicative character ψ is given by

$$G(\psi) = \sum_{s=1}^{p-1} \psi(\varpi(s)) z^{2s} \in \mathbf{Z}[\mu_{p-1}][z]/(z^{4p}-1)$$

as above. Note also that $(1+z^{2p})^2 = 2(1+z^{2p})$.

Hence, squaring formula (9), we get

$$16A_v^2 = 2(p-2)T + 2(1+z^{2p})\mathscr{E}_v,$$

where

$$\begin{aligned}\mathscr{E}_v = 1 &- 2((-1)^v G(\eta) + \bar{\chi}(c^v)G(\chi) + \chi(c^v)G(\bar{\chi})) + 3(p-1-t)\\ &+ (-1)^v(G(\chi)^2 + G(\bar{\chi})^2) + 2(-1)^v G(\eta)(\bar{\chi}(c^v)G(\chi) + \chi(c^v)G(\bar{\chi})),\end{aligned}$$

using $(1')$ above applied to $\psi = \eta$ and $\psi = \chi$.

By (2′) with $\vartheta = \chi$ and η successively, and $\psi = \chi$, we have

$$G(\chi)^2(1+z^{2p}) = J(\chi,\chi)G(\eta)(1+z^{2p}),$$
$$G(\bar{\chi})^2(1+z^{2p}) = J(\bar{\chi},\bar{\chi})G(\eta)(1+z^{2p}),$$

since $\chi^2 = \bar{\chi}^2 = \eta$ and

$$\bar{\chi}(c^v)G(\eta)G(\chi) + \chi(c^v)G(\eta)G(\bar{\chi})(1+z^{2p})$$
$$= \{\bar{\chi}(c^v)J(\eta,\chi)G(\bar{\chi}) + \chi(c^v)J(\eta,\bar{\chi})G(\chi)\}(1+z^{2p}).$$

As we have seen in the corollary above, $J(\chi,\chi) = \chi(-1)J(\eta,\chi)$. Here $\chi(-1) = 1$ because we have $-1 = c^{(p-1)/2} = (c^4)^{(p-1)/8}$. We define $\pi = a + bi$ by

$$\pi = a + bi = -J(\eta,\chi) = -J(\chi,\chi) \in \mathbf{Z}[i].$$

Then $p = \pi\bar{\pi} = a^2 + b^2$. We give more details on a and b in Section 4.

For now, we proceed to calculate the terms $(A_0^2 - 2A_0) + (A_2^2 - 2A_2)$ and $(A_1^2 - 2A_1) + (A_3^2 - 2A_3)$ using the notation $\pi + \bar{\pi} = 2a$ and setting $t = \sum_{s=1}^{p-1} z^{2s}$ for brevity.

Since $(1+z^{2p})t = (1+z^{2p})\sum_{s=1}^{p-1} z^{2s} = T - (1+z^{2p})$, it follows from the above formulas that, after simplifying a factor 2, we have

$$8A_v^2 = (p-5)T + \{3p + 1 - (-1)^v 2(a+1)G(\eta)\}(1+z^{2p})$$
$$- 2\{\bar{\chi}(c^v)(\bar{\pi}+1)G(\chi) + \chi(c^v)(\pi+1)G(\bar{\chi})\}(1+z^{2p}), \qquad (10)$$

using $\bar{\chi}(c^v) = (-i)^v = (-1)^v\chi(c^v)$.

Since $\chi(c^2) = \bar{\chi}(c^2) = -1$, we have after simplifying another factor 2,

$$4(A_0^2 + A_2^2) = (p-5)T + (3p + 1 - 2(a+1)G(\eta))(1+z^{2p}).$$

Since by formulas (6) and (7) we have

$$8(A_0 + A_2) = 4T + (-4 + 4G(\eta))(1+z^{2p}),$$

we get

$$4\{(A_0^2 - 2A_0) + (A_2^2 - 2A_2)\} = (p-9)T + (3p + 5 - 2(a+3)G(\eta))(1+z^{2p}).$$

Similarly,

$$4\{(A_1^2 - 2A_1) + (A_3^2 - 2A_3)\} = (p-9)T + (3p + 5 + 2(a+3)G(\eta))(1+z^{2p}).$$

In order to evaluate the last two terms in the formula (1) for C, we still have to apply the automorphism

$$\sigma : \mathbf{Z}[i][z]/(z^{4p}-1) \to \mathbf{Z}[i][z]/(z^{4p}-1)$$

defined by $\sigma|_{\mathbf{Z}[i]} = \mathrm{id}$, and $\sigma(z) = iz$.

The effect of σ is given by $\sigma(A_v) = B_v$, $\sigma(T) = U = \sum_{s=0}^{2p-1} (-1)^s z^{2s}$.

Recall that $G(\eta)(1+z^{2p}) = \sum_{s\in S} \left(\frac{s}{p}\right) z^{2s} \in \mathbf{Z}[i][z]/(z^{4p}-1)$, where as above $S = [1, p-1] \cup [p+1, 2p-1]$.

Applying σ, we obtain by an easy calculation

$$G(\eta)(1+z^{2p}) - \sigma[G(\eta)(1+z^{2p})] = 2\sum_{s=1}^{p-1} \eta(s) z^{2s+\varepsilon(s)},$$

where $\varepsilon(s) = (1+(-1)^s)p$.

It follows, using formula (1), that

$$C = 4p + (p-9)\sum_{s=1}^{p-1} z^{4s} - 2(a+3)\sum_{s=1}^{p-1} \eta(s) z^{2s+\varepsilon(s)}.$$

Regrouping the coefficients of z^k and z^{-k} and observing that evidently $\varepsilon(s) + \varepsilon(p-s) = 2p$, we can write this as

$$\begin{aligned} C = 4p &+ (p-9)\sum_{s=1}^{(p-1)/2} (z^{4s} + z^{-4s}) \\ &- 2(a+3)\sum_{s=1}^{(p-1)/2} \eta(s)(z^{2s+\varepsilon(s)} + z^{-(2s+\varepsilon(s))}). \end{aligned} \tag{11}$$

Note that in these expressions the exponents of z are all distinct and even.

A similar calculation yields

$$2(A_0^2 - A_2^2) = -\{(\pi+1)G(\bar{\chi}) + (\bar{\pi}+1)G(\chi)\}(1+z^{2p}).$$

Since on the other hand, we have

$$4(A_0 - A_2) = 2\{G(\chi) + G(\bar{\chi})\}(1+z^{2p}),$$

it follows from formula (2) that

$$C_{0,1} = \{(\bar{\pi}+3)G(\chi) + (\pi+3)G(\bar{\chi})\}(z^p + z^{-p}).$$

Denoting by Γ_v' the intersection

$$\Gamma_v' = \Gamma_v \cap [1, p-1],$$

an easy calculation yields

$$C_{0,1} = \left\{ \sum_{s \in \Gamma'_0 \cup \Gamma'_2} 2(a+3)\sigma(s) z^{2s} + \sum_{s \in \Gamma'_1 \cup \Gamma'_3} 2b\sigma(s) z^{2s} \right\} (z^p + z^{-p}),$$

where

$$\sigma(s) = \begin{cases} +1 & \text{if} \quad s \in \Gamma'_0 \cup \Gamma'_1, \\ -1 & \text{if} \quad s \in \Gamma'_2 \cup \Gamma'_3. \end{cases}$$

Regrouping the coefficients of z^k and z^{-k} and using the notation

$$\Gamma''_v = \Gamma_v \cap \left[1, \frac{p-1}{2}\right],$$

we can write this as

$$\begin{aligned} C_{0,1} = {} & 2(a+3) \sum_{s \in \Gamma''_0 \cup \Gamma''_2} \sigma(s) \{ z^{p-2s} + z^{-(p-2s)} + z^{p+2s} + z^{-(p+2s)} \} \\ & + 2b \sum_{s \in \Gamma''_1 \cup \Gamma''_3} \sigma(s) \{ z^{p-2s} + z^{-(p-2s)} + z^{p+2s} + z^{-(p+2s)} \}. \end{aligned} \tag{12}$$

Here, the exponents of z in the expression for $C_{0,1}$ are all odd and distinct. Observe also that the exponents p and $-p$ are absent. Hence, $\gamma_p = 0$. Thus, all periodic correlations of $F(z)$ are as announced in the theorem. This finishes the proof of Theorem 1. ∎

4. PROOF OF THEOREM 2

We start by giving the explicit formula for $\pi = a + bi = -J(\eta, \chi)$ in terms of $\Gamma = \ker(\chi)$, for every prime $p \equiv 1 \bmod 4$.

We have $J(\eta, \chi) = \sum_{x \in \mathbf{F}_p^* \setminus \{-1\}} \eta(-x)\chi(1+x) = \sum_{x \in \mathbf{F}_p^* \setminus \{-1\}} \left(\frac{x}{p}\right)\chi(1+x)$ by definition, where χ is the biquadratic character considered above.

Therefore $\pi = -J(\eta, \chi)$ may be written

$$\begin{aligned} \pi = {} & - \sum_{x \in \Gamma \setminus \{-1\}} \left(\frac{1+x}{p}\right) - i \sum_{x \in \Gamma} \left(\frac{1+cx}{p}\right) + \sum_{x \in \Gamma} \left(\frac{1+c^2 x}{p}\right) \\ & + i \sum_{x \in \Gamma} \left(\frac{1+c^3 x}{p}\right). \end{aligned}$$

On the other hand, the well-known formulas (see [Ha, Lemma 14.1.1])

$$\sum_{x\in\mathbf{F}_p^*}\left(\frac{x}{p}\right)=0 \quad \text{and} \quad \sum_{x\in\mathbf{F}_p^*}\left(\frac{x}{p}\right)\left(\frac{1+x}{p}\right)=-1$$

produce the following 2 equations:

$$\sum_{x\in\Gamma\setminus\{-1\}}\left(\frac{1+x}{p}\right)+\sum_{x\in\Gamma}\left(\frac{1+cx}{p}\right)+\sum_{x\in\Gamma}\left(\frac{1+c^2x}{p}\right)+\sum_{x\in\Gamma}\left(\frac{1+c^3x}{p}\right)=-1,$$

$$\sum_{x\in\Gamma\setminus\{-1\}}\left(\frac{1+x}{p}\right)-\sum_{x\in\Gamma}\left(\frac{1+cx}{p}\right)+\sum_{x\in\Gamma}\left(\frac{1+c^2x}{p}\right)-\sum_{x\in\Gamma}\left(\frac{1+c^3x}{p}\right)=-1.$$

It follows that

$$\sum_{x\in\Gamma\setminus\{-1\}}\left(\frac{1+x}{p}\right)+\sum_{x\in\Gamma}\left(\frac{1+c^2x}{p}\right)=-1, \sum_{x\in\Gamma}\left(\frac{1+cx}{p}\right)+\sum_{x\in\Gamma}\left(\frac{1+c^3x}{p}\right)=0$$

and therefore

$$\pi=a+bi=-\left\{2\sum_{x\in\Gamma\setminus\{-1\}}\left(\frac{1+x}{p}\right)+1\right\}-2i\sum_{x\in\Gamma}\left(\frac{1+cx}{p}\right).$$

Assume now $p\equiv 1 \bmod 8$. Recall that the correlations γ_k in Theorem 1 all belong to the set $\{0, p-9, \pm 2(a+3), \pm 2b\}$. We will derive from the above formula for π the congruences

$$a\equiv 1 \bmod 4 \qquad \text{and} \qquad b\equiv 0 \bmod 4,$$

implying $\gamma_k\equiv 0 \bmod 8$ for all $k=1,\ldots,2p-1$.

For $x\in\Gamma\setminus\{-1\}$, we have $(\frac{1+x}{p})=\pm 1$. Also $(\frac{1+cx}{p})=\pm 1$ because $-c^{-1}\notin\Gamma$. Since $p\equiv 1 \bmod 8$, the order $\frac{p-1}{4}$ of Γ is even, thus $|\Gamma\setminus\{-1\}|$ is odd, and it follows that we have

$$a=-\left\{2\sum_{x\in\Gamma\setminus\{-1\}}\left(\frac{1+x}{p}\right)+1\right\}\equiv 1 \bmod 4$$

and

$$b=-2\sum_{x\in\Gamma}\left(\frac{1+cx}{p}\right)\equiv 0 \bmod 4.$$

These congruences, together with the correlations formulas in Theorem 1, show that the circulant matrices we obtain in that theorem are indeed enhanced 8-modular Hadamard matrices.

To complete the proof of Theorem 2, it remains to characterize the primes $p \equiv 1 \bmod 8$ for which all the correlations γ_k vanish modulo 16.

We observe first that since $\gamma_{4j} = p - 9$ for $j = 1, \ldots, \frac{p-1}{2}$ we must have $p \equiv 9 \bmod 16$. Next, since $a \equiv 1 \bmod 4$ and $b \equiv 0 \bmod 4$, it follows from $p = a^2 + b^2 \equiv 9 \bmod 16$ that $a \equiv -3 \bmod 8$. Thus the correlations $\pm 2(a+3)$ vanish modulo 16.

The correlations γ_k are therefore all divisible by 16 for $k = 1, \ldots, 2p-1$ if and only if $p \equiv 9 \bmod 16$ and $b \equiv 0 \bmod 8$.

Now, it suffices to appeal to the theorem of Gauss: The odd prime p can be written as $p = A^2 + 64B^2$ if and only if 2 is a fourth power mod p.

It follows that the polynomial $F(z)$ of Theorem 1 yields a circulant enhanced 16-modular Hadamard matrix of size $4p$ if and only if

$$p \equiv 9 \bmod 16 \text{ and } 2 \text{ is a fourth power modulo } p.$$

Note that clearly 2 is a fourth power in $\mathbf{F}_p^*$ if and only if $2^{(p-1)/4} \equiv 1 \bmod p$.

This finishes the proof of Theorem 2. ∎

A simple proof of the theorem of Gauss we have just used was given by Lejeune Dirichlet [D] in 1857. It uses only quadratic reciprocity.

Reference [Ho, Vol. I, p. 91] contains a variant of the proof which is attributed by the author to A. Aigner, and is also quite elementary. Another good exposition of the theorem is given in [BEW, p. 225].

Here is a brief account, based on Holzer's proof:

THEOREM (Gauss). *Let p be a prime congruent to* $1 \bmod 8$. *The equation $x^4 = 2$ is solvable in the prime field $\mathbf{F}_p$ if and only if p can be written as $p = a^2 + b^2$ with b divisible by* 8.

The congruence $p \equiv 1 \bmod 8$ implies that p may be represented as $p = a^2 + b^2 = r^2 + 2s^2$ with a, b, r, s integers.

We will use Jacobi symbols $(\frac{m}{n})$ defined for n positive and odd. By definition,

$$\left(\frac{m}{n}\right) = \prod_{i=1}^{i=k} \left(\frac{m}{p_i}\right),$$

where $n = p_1 \cdots p_k$ is the decomposition of n as a product of (odd, not necessarily distinct) primes, and $(\frac{m}{p_i})$ is the Legendre symbol.

The symbol $(\frac{m}{n})$ depends only on the class of m modulo n and satisfies the familiar formulas of quadratic reciprocity

$$\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}, \qquad \left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8},$$
$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{(m-1)/2\,(n-1)/2}.$$

If m is a square modulo n, then $(\frac{m}{n}) = +1$. The converse, however, does not hold unless n is a prime.

For the proof of the theorem, note first that r is odd and $(\frac{r}{p}) = (-1)^{(r^2-1)/8}$. Indeed,

$$\left(\frac{r}{p}\right) = \left(\frac{p}{r}\right) = \left(\frac{r^2+2s^2}{r}\right) = \left(\frac{2s^2}{r}\right) = \left(\frac{2}{r}\right) = (-1)^{(r^2-1)/8}.$$

In order to calculate $(\frac{s}{p})$, set $s = 2^v s'$ with s' odd. We have

$$\left(\frac{s'}{p}\right) = \left(\frac{p}{s'}\right) = \left(\frac{r^2+2s^2}{s'}\right) = \left(\frac{r^2}{s'}\right) = 1.$$

Since $(\frac{2}{p}) = 1$, it follows $(\frac{s}{p}) = 1$.

Set $t = \frac{r}{s} \bmod p$. The equation $p = r^2 + 2s^2$ shows that $t^2 \equiv -2 \bmod p$. Since -1 is a fourth power modulo p, we conclude that

2 *is a fourth power modulo p if and only if t is a square mod p, i.e. if and only if* $(\frac{t}{p}) = +1$.

Now, $(\frac{t}{p}) = (\frac{rs}{p}) = (\frac{r}{p}) = (-1)^{(r^2-1)/8}$.

On the other hand, the equation $a^2 - 2s^2 = r^2 - b^2 = (r+b)(r-b)$ shows that 2 is a square modulo $r-b$ (and modulo $r+b$) which is odd. Hence,

$$\left(\frac{2}{r-b}\right) = 1.$$

By quadratic reciprocity, $(\frac{2}{m}) = (-1)^{(m^2-1)/8}$, it follows that $(\frac{2}{m}) = 1$ is equivalent to $m \equiv \pm 1 \bmod 8$.

Thus, $r - b \equiv \pm 1 \bmod 8$. On the other hand, the equation $p = a^2 + b^2$ with $p \equiv 1 \bmod 8$ implies $b \equiv 0 \bmod 4$. Therefore, the two conditions

$$r \equiv \pm 1 \bmod 8 \text{ and } b \equiv 0 \bmod 8$$

are equivalent. (The other case is $r \equiv \pm 3 \bmod 8$ and $b \equiv 4 \bmod 8$.)

Since, $(\frac{t}{p}) = (-1)^{(r^2-1)/8} = 1$ is also equivalent to $r \equiv \pm 1 \bmod 8$, it follows that 2 is a fourth power if and only if $b \equiv 0 \bmod 8$.

ACKNOWLEDGMENT

During the preparation of this paper, the first author has partially benefited from a research contract with the Fonds National Suisse pour la Recherche Scientifique.

REFERENCES

[BEW] B. Berndt, R. Evans, and K. Williams, "Gauss and Jacobi Sums," Canadian Mathematical Society Series of Monographs and Advanced Texts, Vol. 21, Wiley–Interscience, New York, 1998.

[D] G. L. Dirichlet, Über den biquadratischen Charakter der Zahl "Zwei," Werke, Bd. II, 260, or *Crelle's J.*, Bd. 57 (1860), 187–188.

[EK1] S. Eliahou and M. Kervaire, Modular sequences and modular Hadamard matrices, *J. Combin. Des.* **9** (2001), 187–214.

[EK2] S. Eliahou and M. Kervaire, Circulant modular Hadamard matrices, *Ens. Math.* **47** (2001), 103–114.

[Ha] M. Hall, "Combinatorial Theory," 2nd Ed., Wiley, New York, 1986.

[Ho] L. Holzer, "Zahlentheorie," Teubner, Leipzig, 1958.

[IR] K. Ireland and M. Rosen, "A Classical Introduction to Modern Number Theory," 2nd Ed., Graduate Text in Mathematics, Vol. 84, Springer-Verlag, Berlin, 1992.

[MB1] O. Marrero and A. T. Butson, Modular Hadamard matrices and related designs, *J. Combin. Theory A* **15** (1973), 257–269.

[MB2] O. Marrero and A. T. Butson, Modular Hadamard matrices and related designs, II, *Canad. J. Math.* **XXIV** (1972), 1100–1109.